Keynote Address
Vulnerability Management Best Practices

Brian Kenyon - Foundstone Security, McAfee

2005 Annual Security Conference
Digital Citizenship - Utah at Risk

March 7 - 8, 2005

Utah! Where ideas connect™

Sponsored by

UEN UTAH EDUCATION NETWORK WWW.UEN.ORG

UTAH STATE OFFICE OF EDUCATION

ITS Customer Driven Technology Information Technology Services

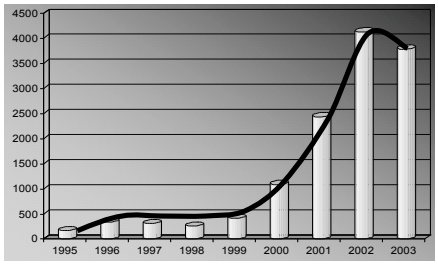
McAfee

Vulnerability Best Practices

www.foundstone.com

McAfee

Vendor vulnerabilities on the rise

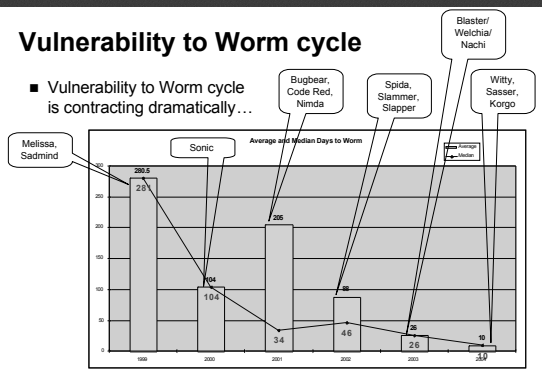


Source: CERT

McAfee

Vulnerability to Worm cycle

- Vulnerability to Worm cycle is contracting dramatically…



McAfee

Will vulnerabilities ever go away?

- If, 95-99% of all attacks come from known vulnerabilities and misconfigurations [Carnegie Mellon]
- And, vulnerabilities are on the rise
- And, known vulnerabilities and mis-configurations come from human error
- And, for the foreseeable future, humans will be the creators and maintainers of technology
- **Then, vulnerabilities (and risk) are here to stay!**

McAfee

Technology	Vulnerability Related?
NIDS/HIDS	Detecting attackers taking advantage of *vulnerabilities*.
NIPS/HIPS	Detecting and preventing attackers from taking advantage of *vulnerabilities*.
Firewalls/VPN	Blocking attackers taking advantage of *vulnerabilities.*
Patch Management	Fixing *vulnerabilities*.
Anti-virus	Finding and fixing *vulnerabilities*.
Event Correlation	Managing logs/events of attacks (based on *vulnerabilities).*
Policy Management	Ensuring compliance to prevent attacks on *vulnerabilities*.
Encryption	Securing clear-text data (*a vulnerability*).
Content/Email Filtering	Preventing content/email with *vulnerabilities*.
VA/VM & Risk Mgmt.	Discovering and managing *vulnerabilities* and associated risk.

McAfee

What does the future hold?

- Zero-day worm categorization
  - Type I: vendor knows of the vulnerability but hasn't released the patch yet (shortest)
  - Type II: vendor doesn't know of the vulnerability (long)
  - Type III: vendor doesn't know of the vulnerability and it hits an EOL product such as Windows 98/NT 4.0 (longest)
- Type III scares me to death!

McAfee

So What Can We Do???

- Risk Management Strategies include:
  - Risk Transfer
    - Contractual transfer to 3rd party
    - Insurance provider
  - Risk Avoidance
    - Eliminate existing exposures/capabilities
  - Risk Acceptance
    - Security spending has a point of diminishing returns, some risk is easier to accept
  - Risk Mitigation
    - Security countermeasures (people/process/technology)

McAfee

Depends on your philosophy…

- Would you rather affect the symptoms? Or the problem?
  - The cold/flu medication business is much more lucrative than the vaccine business
- Products alone only affect the symptoms…
- Services/products/education in combination, affect the core problem…

McAfee

What is Vulnerability Management?

www.foundstone.com

McAfee

Gartner on Vulnerability Management

"Vulnerability management is a set of processes and technologies that are used to:

- **Establish and maintain a security configuration baseline**
- **Discover, prioritize and mitigate vulnerabilities**
- **Establish security controls**
- **Eliminate root causes"**

"Enterprises that implement a vulnerability management process will experience 90 percent fewer successful attacks…"

-- Mark Nicolett, Gartner
Dec '03

McAfee

What Is Vulnerability Management?

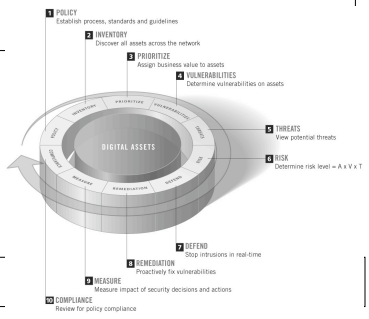
■ At a high level, the intelligent confluence of…

Assessment	**+**	**Analysis**	**+**	**Remediation**
What assets?		What to fix first?		Fix & verify it's fixed!

- Component of Risk Management
- Balance the demands of business goals and processes

McAfee

Vulnerability Management Lifecycle



McAfee

Asset Inventory and Prioritization

- Inventory Assets
  - All hosts, services, operating systems, asset owner
  - Regular, automated updates
  - Combination of network and agent based technologies
- Create an Asset Criticality Profile (ACP)
  - Data Classification
  - Business process that is supported
  - Environment (Internet vs. Intranet)

McAfee

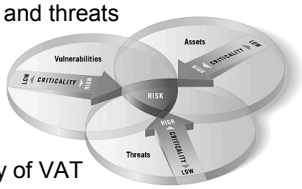
Identify Vulnerabilities and Threats

- Traditional vulnerability assessment
  - Integrate with asset inventory for measurement
  - Regular, automated schedule
- Monitor Threats
  - Track viruses, worms, internal and external threats
  - Map threat environment to existing asset vulnerability inventory

McAfee

Prioritize Remediation based on Risk

- Identify vulnerabilities and threats
- The Union of:
  - Vulnerabilities
  - Assets
  - Threats
- Based on the criticality of VAT
- Focus your resources on the TRUE risk



McAfee

Remediation / Resolution

- Apply the Pareto Principle – the 80/20 rule
  - Focus on the vital few not the trivial many
  - 80% of your risk can be eliminated by addressing 20% of the issues
  - The Risk Union will show you the way
    - Right assets
    - Relevant threats
    - Critical vulnerabilities

McAfee

Measure

- Current State of security metrics
  - You can't manage what you can't measure
  - No focus on quantifying "Security"
  - No taxonomy of security
    - The terms risk, criticality, impact, threats are all perverted
    - There is no common definition that is widely adopted
  - Return on Security Investment (ROSI) is extremely difficult to calculate
  - No accountability in security

McAfee

Measure

- Future Look:
  - Accountability
  - A universal standard to quantify risk
  - Common nomenclature
  - The use of IRR and NPV calculations for budgeting purposes will increase
  - Dashboard view of assets, vulnerabilities, and threats across disparate organizations
  - Technologies will help answer the questions:
    - Am I secure
    - Who is accountable and by when
    - Am I getting better or worse
    - How am I trending over time
    - How do I compare to my peers

McAfee

Training & Communication

- Knowledge is the Foundation
  - External and Internal Resources
  - Security Intelligence
  - Understanding before Reacting
- Centralized Communication
  - Exec to Tech Reporting
  - Justifying the Security Expense

McAfee

Conclusions

- All assets are not created equally
- You cannot respond to or even protect against all threats
- An effective vulnerability management program focuses on Risk
  - Vulnerabilities + Assets + Threats
- VM is truly preventative and proactive, not reactive
- Finds and fixes the core problems, not the symptoms
- No other form of security is as effective in reducing risk than vulnerability management